Cyclic Subgroups of the Simple Ternary Linear Fractional Group in a Galois Field.

BY L. E. DICKSON.

1. The present paper is an addition to the writer's article (*American Journal,* vol. XXII, pp. 231–252). It gives proofs of the results there stated in §§13–14 (pp. 249–251) and certain new theorems related to them. The question concerns the substitutions

$$x' = \alpha^r x, \quad y' = \alpha^s y, \quad z' = \alpha^{-r-s} z, \tag{1}$$

where α is a primitive root of the Galois Field of order p^n. Two cases arise according to the value of the greatest common divisor d of 3 and $p^n - 1$.

2. Suppose first that $d = 1$. The substitutions (1) are all powers of certain substitutions C of period $p^n - 1$ and having the form (1) in which the greatest common divisor $[r, s, p^n - 1]$ of $r, s, p^n - 1$ is unity. The cyclic group generated by C contains* $\phi(p^n - 1)$ substitutions of period $p^n - 1$. To determine which of them are conjugate under linear transformation, we must find when the powers C^a and C^b, where a and b are prime to $p^n - 1$, have the same sets of multipliers [the coefficients of x, y, z in (1)]. If a_1 be determined so that $aa_1 \equiv 1 \pmod{p^n - 1}$, whence $C^{aa_1} = C$, then C^a and C^b have the same multipliers if, and only if, C and C^{ba_1} do. It, therefore, suffices to determine when C and C^m have the same multipliers, where m is prime to $p^n - 1$ and $1 < m < p^n - 1$. But the sets of multipliers

$$\alpha^r, \alpha^s, \alpha^{-r-s}; \quad \alpha^{mr}, \alpha^{ms}, \alpha^{-mr-ms}$$

are identical apart from their order only in three cases:

(a). $\alpha^{mr} = \alpha^r, \alpha^{ms} = \alpha^s$. Then $r(m-1)$ and $s(m-1)$ are divisible by

---

* As usual, $\phi(m)$ denotes the number of integers $< m$ which are prime to m.

$p^n - 1$. Since $[r, s, p^n - 1] = 1$, this requires that $m - 1$ be divisible by $p^n - 1$, contrary to the hypothesis $1 < m < p^n - 1$.

(b). $\alpha^{mr} = \alpha^s$, $\alpha^{ms} = \alpha^r$. We have the congruences modulo $p^n - 1$:

$$mr \equiv s, \quad ms \equiv r, \quad m^2 r \equiv r, \quad m^2 \equiv 1.$$

The fourth follows from the third, since $[r, s, p^n - 1] = 1$, so that r and s must each be prime to $p^n - 1$. Inversely, if m be any solution of $m^2 \equiv 1 \pmod{p^n - 1}$, and if r be any integer less than and prime to $p^n - 1$, and if s be determined by $s \equiv mr \pmod{p^n - 1}$, then C and C^m have the same multipliers. Moreover, C is the r^{th} power of a substitution with the multipliers α, α^m, α^{-1-m}.

(c). $\alpha^{mr} = \alpha^s$, $\alpha^{ms} = \alpha^{-r-s}$, $\alpha^{-mr-ms} = \alpha^r$. Hence, if $M \equiv m^2 + m + 1$, both rM and sM, and consequently also M, are multiples of $p^n - 1$. Since $m(m+1)$ is even, M is an odd number. Hence, $p^n - 1$ must be odd, so that p^n is even and therefore $p = 2$. The condition $M \equiv 0$ is equivalent to

$$(2m+1)^2 \equiv -3, \qquad \pmod{p^n - 1}.$$

But* -3 is a quadratic residue of $p^n - 1$ if, and only if, the latter be not divisible by 8, 9 or any prime of the form $6l + 5$. Since $d = 1$, $p^n - 1 = 3^n - 1$ or $3l + 1$, the factor 3 cannot occur in $p^n - 1$. Also n must be odd since $2^{2t} - 1$ is divisible by 3. *Hence, solutions m occur if, and only if, $p^n = 2^n$, n odd, and such that the prime factors of $2^n - 1$ are all of the form $6k + 1$.*

If m be a solution of $x^2 + x + 1 \equiv 0 \pmod{2^n - 1}$, so is also $-1 - m$. If $-1 - m \equiv m$, then $m \equiv -\frac{1}{2}$, requiring $\frac{3}{4} \equiv 0 \pmod{2^n - 1}$, whereas 3 is prime to $2^n - 1$, n odd. Hence, the solutions give rise, in sets of two, to the same substitution. The resulting substitution is the r^{th} power of a substitution having the multipliers α, α^m, α^{-1-m}. The latter substitutions belong to different cyclic groups; for, $(\alpha^m)^k = \alpha$ requires that $k = -1 - m$.

It follows that the substitutions (1) all belong to the four types of cyclic groups of order $p^n - 1$ given on p. 250 of the earlier paper.

As a first example, let $p^n = 8$. There is one and but one cyclic group of each of the classes (i), (ii), (iii), and none of class (iv). The generators have respectively the sets of multipliers:

$$\alpha,\ \alpha^{-1},\ 1; \quad \alpha,\ \alpha^2,\ \alpha^{-3}; \quad \alpha,\ \alpha,\ \alpha^{-2}.$$

---

* Gauss, "Disquisitiones Arithmeticae," Art. 120.

As a second example, let $p^n = 17$. Then $m^2 \equiv 1 \pmod{16}$ has the solutions $(m > 1)$ -1, 7 and 9, giving the sets of multipliers,

$$\alpha, \alpha^{-1}, 1; \quad \alpha, \alpha^7, \alpha^8; \quad \alpha, \alpha^9, \alpha^6.$$

The two cyclic groups of class (iv) are determined by the multipliers

$$\alpha, \alpha^2, \alpha^{13}; \ \alpha, \alpha^3, \alpha^{12}.$$

3. Suppose next that $d = 3$, so that $p^n = 3t + 1$. Denote by Σ the homogeneous substitution with the multipliers $\alpha^t, \alpha^t, \alpha^t$. The quotient-group is obtained from the homogeneous group by making Σ correspond to the identity. Hence the set of exponents r, s, $-r-s$ in the substitution (1) may be replaced by the set $r+t$, $s+t$, $-r-s+t$ or by the set $r+2t$, $s+2t$, $-r-s+2t$, so that the exponents may be taken modulo t.

If t be prime to 3, each substitution (1) *is a power of some substitution of the form* (1) *and having the period $p^n - 1$.*

We may suppose that r and s are relatively prime; for if they have a common divisor g, the substitution (1) is the g^{th} power of a similar substitution. Hence one of the two, say r, is prime to $p^n - 1$. An integer r_1 may therefore be determined so that $rr_1 = 1 \pmod{p^n - 1}$, whence s/r is congruent to $sr_1 \equiv \rho$. Then $C = C_1^r$, where C_1 has the multipliers $\alpha, \alpha^\rho, \alpha^{-1-\rho}$ and is of period τ, the least integer such that $\tau(\rho - 1)$ and $\tau(\rho + 2)$ are divisible by $p^n - 1$. Hence $\tau = p^n - 1$ if, and only if, $\rho - 1$ is prime to 3. The theorem is therefore proved except for the case $\rho = 3l + 1$, when C_1 has the form

$$C_1: \quad x' = \alpha x, \qquad y' = \alpha^{3l+1} y, \qquad z' = \alpha^{-3l-2} z.$$

In the quotient-group, C_1 is of period $t = \frac{1}{3}(p^n - 1)$.

If, now, t be prime to 3, either t itself or else $2t$ will have the form $3m - 1$, so that $9m - 3$ is a multiple of $p^n - 1$. Either ΣC_1 or else $\Sigma^2 C_1$ has the form

$$x' = \alpha^{3m} x, \qquad y' = \alpha^{3m+3l} y, \qquad z' = \alpha^{3m-3l-3} z \equiv \alpha^{21m-3l-9} z,$$

which is the cube of the substitution of determinant unity,

$$x' = \alpha^m x, \qquad y' = \alpha^{m+l} y, \qquad z' = \alpha^{7m-l-3} z. \tag{2}$$

If l be not divisible by 3, the difference of the first two exponents in (2) is prime to 3 and therefore (2) is a power of a substitution of period $p^n - 1$. If l be divi-

sible by 3, C_1 is identical in the quotient-group with the substitution having the multipliers

$$\alpha^{3m}, \quad \alpha^{3m+3l} \equiv \alpha^{12m+3l-3}, \quad \alpha^{3m-3l-3} \equiv \alpha^{12m-3l-6}$$

and hence is the cube of the substitution of determinant unity

$$x' = \alpha^m x, \quad y' = \alpha^{4m+l-1} y, \quad z' = \alpha^{4m-l-2} z.$$

The difference of the first two exponents being prime to 3, this substitution, and therefore also C, is a power of one of period $p^n - 1$.

4. THEOREM.—*If t be divisible by* 3, *the substitution C_1 is contained in no cyclic group generated by a substitution* (1) *of period $p^n - 1$.*

Suppose that $C_1 = C^q$, C being a substitution of period $p^n - 1$ of the form (1). Since C_1 is of period t, the product tq must be divisible by $p^n - 1 \equiv 3t$. Hence q must be divisible by 3, so that $C_1 = S^3$, $S \equiv C^{q/3}$. Let S, when expressed in the form (1), have s as one of its exponents. Hence $3s \equiv 1 \pmod{t}$, whereas t is supposed to be divisible by 3.

5. The period of a substitution (1) is the least integer τ such that

$$\tau r \equiv \tau s \equiv \tau(-r-s), \qquad \pmod{p^n - 1}$$

Hence $\tau = p^n - 1$ if, and only if, $[r - s, 2r + s, p^n - 1] = 1$.* The condition may also be written $[r - s, 3r, p^n - 1] = 1$. For $d = 3$, $p^n - 1$ is divisible by 3. *Hence, for $d = 3$, a substitution* (1) *is of period $p^n - 1$ in the quotient-group if, and only if, $[r, s, p^n - 1] = 1$ and $r - s$ is prime to* 3.

We proceed to enumerate the number of substitutions P which are of the form (1) and have the period $p^n - 1$. In the notations of the earlier paper, p. 249, there are $\phi(p^n - 1)\,\psi(p^n - 1)$ sets of solutions r, s, each $< p^n - 1$, of $[r, s, p^n - 1] = 1$. We must exclude the E sets r, s for which $r - s$ is divisible by 3. Evidently E equals the number of sets of solutions r, s (mod $3t$) of $[r, s, 3t] = 1$ for which $r = s + 3k$, where the integer k may be taken modulo t. Hence E is the number of sets of solutions k (mod t) and s (mod $3t$) of $[3k, s, 3t] = 1$, equivalent to the pair of conditions $[k, s, t] = 1$, $s \not\equiv 0 \pmod{3}$. Now $[k, \sigma, t] = 1$ has $\phi(t)\,\psi(t)$ sets of solutions k, σ (mod t). Since s is to be determined modulo

* The greatest common divisor of a, b, c is designated $[a, b, c]$.

$3t$ so that $s \equiv \sigma \pmod{t}$ and $s \not\equiv 0 \pmod{3}$, s may equal any of the integers σ, $\sigma + t$, $\sigma + 2t$, not divisible by 3.

If t be prime to 3, one and only one of the integers σ, $\sigma + t$, $\sigma + 2t$ is divisible by 3, so that $E = 2\,\phi(t)\,\psi(t)$. Also

$$\phi(3t) = 2\,\phi(t), \quad \psi(3t) = 4\,\psi(t).$$

Hence there are $6\,\phi(t)\,\psi(t)$ set of integers r, s, each $< 3t$, which lead to substitutions P. No two of the integers r, s, $-r-s$ are equal since their differences are all prime to 3. Allowing for their six permutations and for the equivalence of P, ΣP and $\Sigma^2 P$ in the quotient-group, *we obtain* $\frac{1}{3}\,\phi(t)\,\psi(t)$ *sets of multipliers giving non-conjugate substitutions of period* $p^n - 1$ *in the quotient-group.*

For example, if $p^n = 13$, there are four non-conjugate substitutions of period 12 in the quotient-group. Their sets of multipliers are

$$\alpha,\ \alpha^2,\ \alpha^9;\ \ \alpha,\ \alpha^3,\ \alpha^8;\ \ \alpha,\ \alpha^{-1},\ 1;\ \ \alpha^2,\ \alpha^3,\ \alpha^7.$$

If t be divisible by 3, all or none of the integers σ, $\sigma + t$, $\sigma + 2t$ are divisible by 3, according as σ is or is not divisible by 3. Hence $E = 3\,E'$, where E' denotes the number of sets of solutions k, $\sigma \pmod{t}$ of $[k, \sigma, t] = 1$, $\sigma \not\equiv 0 \pmod{3}$. Let $3, q_1, q_2, \ldots.$ denote the distinct prime factors of t. Of the $\frac{2}{3}t^2$ sets of two integers k, σ, each $< t$, with σ prime to 3, $\frac{2}{3}t^2/q_i^2$ sets have k and σ both multiples of q_i with σ prime to 3, $\frac{2}{3}t^2/q_i^2 q_j^2$ sets have k and σ both multiples of $q_i q_j$ with σ prime to 3, etc. Hence

$$E' = \tfrac{2}{3}\left\{t^2 - \sum_i \frac{t^2}{q_i^2} + \sum_{i,j} \frac{t^2}{q_i^2 q_j^2} - \sum_{i,j,k} \frac{t^2}{q_i^2 q_j^2 q_k^2} + \ldots.\right\}.$$

Let $t = T\,3^\tau$, where T is prime to 3. Then the distinct prime factors of T are $q_1, q_2, \ldots.$, so that

$$F(T) \equiv \phi(T)\,\psi(T) \equiv T^2 - \sum_i \frac{T^2}{q_i^2} + \sum_{i,j} \frac{T^2}{q_i^2 q_j^2} - \ldots.$$

Hence

$$E' = \tfrac{2}{3}\,t^2\,T^{-2}\,F(T) = 2.3^{2\tau-1}\,F(T),$$

$$\phi(p^n - 1)\,\psi(p^n - 1) = F(3t) = F(3^{\tau+1})\,F(T) = 8.3^{2\tau}\,F(T).$$

Excluding the $E = 3\,E'$ sets, there remain $6.3^{2\tau}F(T)$ sets of integers r, s, each $< 3t$, which lead to substitutions P.

If $t = 3^\tau\,T$, $\tau \geqq 1$, *there are* $M \equiv 3^{2\tau-1}\,F(T)$ *non-conjugate substitutions of period* $p^n - 1$ *in the quotient-group.*

For example, if $p^n = 19$, the $M = 9$ sets of multipliers leading to non-conjugate substitutions of period 18 are

$$\alpha, \alpha^{-1}, 1; \quad \alpha^5, \alpha^{-5}, 1; \quad \alpha^7, \alpha^{-7}, 1 \quad ; \quad \alpha, \alpha^2, \alpha^{-3}; \quad \alpha^5, \alpha^{10}, \alpha^3 \quad ;$$
$$\alpha^7, \alpha^{14}, \alpha^{-3}; \quad \alpha^{11}, \alpha^4, \alpha^3; \quad \alpha^{13}, \alpha^8, \alpha^{-3}; \quad \alpha^{-1}, \alpha^{-2}, \alpha^3.$$

The first three sets lead to substitutions belonging to the same cyclic group of order 18; likewise for the last six sets.

6. We next determine the cyclic groups of order $p^n - 1$ for the case $p^n - 1 = 3t$, t being prime to 3. Let C denote a substitution (1) in which $[r, s, 3t] = 1$ and $r - s$ is prime to 3. We seek the values of $m > 1$, m being less than and prime to $p^n - 1$, for which C and C^m are conjugate in the quotient-group. Since they must have the same multipliers, α^{mr}, α^{ms}, α^{-mr-ms} must be identical in some order with

$$\alpha^{r+ct}, \quad \alpha^{s+ct}, \quad \alpha^{-r-s+ct}, \qquad (c = 0, 1, \text{ or } 2).$$

Since r and s do not have a factor in common with $p^n - 1$ and enter into the multipliers symmetrically, we may suppose that r is prime to $p^n - 1$. Three cases arise.

(a). If $\alpha^{mr} = \alpha^{r+ct}$, $\alpha^{ms} = \alpha^{s+ct}$, then $(r-s)(m-1)$ is divisible by $p^n - 1$, so that $m - 1$ is divisible by 3. Since $r(m-1)$ and $s(m-1)$ are divisible by t, so is also $m - 1$. Hence, $m - 1$ must be divisible by $3t = p^n - 1$, whereas, $m - 1 < p^n - 1$. The case is, therefore, excluded.

(b). If $\alpha^{mr} = \alpha^{s+ct}$, $\alpha^{ms} = \alpha^{r+ct}$, then $(m+1)(r-s)$ is divisible by $p^n - 1$, so that $m + 1$ is divisible by 3. Also,

$$m^2 r \equiv ms + mct \equiv r + (m+1)ct \equiv r \qquad (\text{mod } 3t).$$

Hence $m^2 \equiv 1 \pmod{3t}$. For each solution of $x^2 \equiv 1 \pmod{t}$, there exists a single integer m (mod $3t$) such that

$$m \equiv x \pmod{t}, \quad m + 1 \equiv 0 \qquad (\text{mod } 3).$$

Since 3 is a factor of $p^n - 1$ but not of t, there are $2^{\mu+\kappa-1}$ values of m to be considered, μ and κ being defined on p. 250 of the earlier paper.

Inversely, if r be any integer less than and prime to $3t$, and if $s \equiv mr - ct \pmod{3t}$, where c is either of the two residues modulo 3 which make $r - s \equiv ct - (m-1)r$ prime to 3, then C has the same multipliers as $C^m \equiv C^m \Sigma^{cm}$.

Moreover, C is the r^{th} power of the substitution C' having the multipliers $\alpha, \alpha^{m+kt}, \alpha^{-1-m-kt}$, where k is determined from $rk \equiv -c \pmod 3$. It follows from the above determination of c that $m-1+kt$ is prime to 3. Hence, C' is of period p^n-1. For $c\equiv 0$, $k\equiv 0 \pmod 3$, we reach the substitution C_1' with the multipliers $\alpha, \alpha^m, \alpha^{-1-m}$. The second possible set of multipliers is

$$\alpha,\ \alpha^{m+kt},\ \alpha^{-1-m-kt}, \qquad (k \text{ and } -1-m-kt \text{ prime to } 3),$$

and defines a substitution C_2'. But if j be determined so that $(m-1)j \equiv -k \pmod 3$, we have

$$\begin{aligned} &m+jt \equiv m+kt+mjt, \quad m(m+jt)\equiv 1+mjt, \\ &(-m-1)(m+jt) \equiv -1-m-kt+mjt, \end{aligned} \qquad \pmod{3t}.$$

Hence $C_2' \equiv C_2'\Sigma^{mjt}$ is conjugate with $(C_1')^{m+jt}$. We may, therefore, confine the discussion to the $2^{\mu+\kappa-1}$ substitutions C_m with the multipliers $\alpha, \alpha^m, \alpha^{-1-m}$ where $m^2\equiv 1 \pmod t$, $m+1\equiv 0 \pmod 3$. We next prove that they generate distinct cyclic groups. Indeed, $C_{m_1} = C_m^y$ requires that either α^{my} or else $\alpha^{(-1-m)y}$ shall be identical with α, α^{1+t} or α^{1+2t}. If this be true for α^{my}, then $my\equiv 1 \pmod t$ and, therefore, $y\equiv m \pmod t$, so that $C_{m_1}\equiv C_m^m$ is conjugate with C_m, whence $m_1\equiv m \pmod t$. In the second alternative, $(-1-m)\,y\equiv 1 \pmod t$, so that $m+1$ must be prime to t. Since m^2-1 is divisible by t, so must also $m-1$ be divisible by t, whence $-2y\equiv 1 \pmod t$. Moreover, either α^y or else α^{my} must be identical with one of the quantities $\alpha^{m_1}, \alpha^{m_1+t}, \alpha^{m_1+2t}$, and, therefore, y or else my must be a root of $x^2\equiv 1 \pmod t$. But the latter has no root of the forms $-\frac{1}{2}, -\dfrac{m}{2}$, since 3 is prime to t. *Hence, there are $2^{\mu+\kappa-1}$ distinct cyclic groups of order p^n-1 in each of which the substitutions of period p^n-1 are conjugate in sets of two.* Their substitutions have in all $\frac{1}{2}\phi(p^n-1)\,2^{\mu+\kappa-1}$ distinct sets of multipliers.

(c). If $\alpha^{mr}=\alpha^{s+ct}$, $\alpha^{ms}=\alpha^{-r-s+ct}$, $\alpha^{-mr-ms}=\alpha^{r+ct}$, then

$$mr-s\equiv ms+r+s, \quad (m-1)(r-s)\equiv 3s \qquad \pmod{3t}$$

requires that $m-1$ be divisible by 3. Also,

$$r(m^2+m+1)\equiv(m+2)\,ct\equiv 0 \qquad \pmod{3t}$$

requires that $m^2+m+1\equiv 0 \pmod{3t}$. As in §2, case (c), this congruence has solutions if, and only if, $p^n=2^n$ and the prime factors of $t\equiv\frac{1}{3}(p^n-1)$ are all of the form $6k+1$. Also n must be even and prime to 3, since t is prime to 3.

Inversely, let the δ distinct prime factors of t be all of the form $6k+1$. Then $x^2+x+1\equiv 0 \pmod{t}$ has 2^δ solutions, each of which leads to an unique integer m such that $m\equiv x \pmod{t}$ and $m-1\equiv 0 \pmod{3}$. Also, let r be any integer less than and prime to $3t$, and let $s\equiv mr-ct$, c being either of the two residues 1, 2 modulo 3 which make $r-s\equiv r(1-m)+ct$ prime to 3. Then the multipliers α^r, α^{mr-ct}, $\alpha^{-mr-r+ct}$ of C are identical with those of $C^m\equiv C^m\Sigma^{-ct}$, viz.:

$$\alpha^{mr-ct}, \quad \alpha^{-mr-r-(m+1)ct}, \quad \alpha^{r+(m-1)ct}.$$

Furthermore, C is the r^{th} power of a substitution C_1 with the multipliers

$$\alpha, \; \alpha^{m+kt}, \; \alpha^{-m-1-kt}, \qquad [kr\equiv -c \pmod{3}],$$

Since c is not divisible by 3, the same is true of $m-1+kt$, so that C_1 has the period p^n-1.

If m be a root of $x^2+x+1\equiv 0 \pmod{3t}$, a second root is $-m-1$. Hence C has the same multipliers as C^{-1-m}. Hence, in the cyclic group generated by C, the substitutions of period p^n-1 have the same sets of multipliers in groups of three.

Since $t=6j+1\equiv 1 \pmod{3}$, $t^2\equiv t \pmod{3t}$ and the power $m+t$ of the first C_1 with the multipliers α, α^{m-t}, α^{-m-1+t} gives the second C_1 with the multipliers α, α^{m+t}, α^{-m-1-t}. Hence, there are $2^{\delta-1}$ sets of multipliers α, α^{m-t}, α^{-m-1+t} of substitutions C_1 conjugate with C_1^m, C_1^{-1-m}. A particular C_1 is conjugate only with its m^{th} or $(-1-m)^{\text{th}}$ powers, and is not conjugate with a different C_1. Indeed, $\alpha^{(m-t)y}=\alpha$, α^{1+t} or α^{1+2t} requires $my\equiv 1 \pmod{t}$, whence $y\equiv -1-m \pmod{t}$. *Hence, there are* $2^{\delta-1}$ *distinct cyclic groups of order* p^n-1, *in each of which the substitutions of period* p^n-1 *are conjugate in sets of three.* The number of distinct sets of multipliers involved is $\frac{1}{3}\phi(2^n-1)\,2^{\delta-1}$.

As a first example, consider the least possible value $n=14$ for which cyclic groups of the type considered in case (c) can occur. Then $t=\frac{1}{3}(2^{14}-1)=43\,.\,127$. The $2^{\delta-1}\equiv 2$ cyclic groups of that type are generated by substitutions with the multipliers

$$\alpha, \; \alpha^{1670}, \; \alpha^{-1671}; \quad \alpha, \; \alpha^{1885}, \; \alpha^{-1886}.$$

As a second example, let $p^n=31$, so that $t\equiv 10$ is prime to 3. The quotient-group contains two special cyclic groups of order 30 falling under case (b); indeed, the congruences $m^2\equiv 1 \pmod{10}$, $m+1\equiv 0 \pmod{3}$ give $m\equiv 11$ or $-1 \pmod{30}$. In place of the multipliers α, α^{11}, α^{18}, we may take α^{21}, $\alpha^{31}=\alpha$,

$\alpha^{38} = \alpha^8$. The multipliers of the substitutions of period 30 in the two special cyclic groups are respectively

$$\alpha, \alpha^8, \alpha^{21}; \quad \alpha^7, \alpha^{26}, \alpha^{27}; \quad \alpha^{13}, \alpha^{14}, \alpha^3; \quad \alpha^{19}, \alpha^2, \alpha^9;$$
$$\alpha, \alpha^{-1}, 1; \quad \alpha^7, \alpha^{-7}, 1; \quad \alpha^{13}, \alpha^{-13}, 1; \quad \alpha^{19}, \alpha^{-19}, 1.$$

There are two* general cyclic groups G_{30} generated by substitutions not conjugate with any of their powers. The exponents of the multipliers of their distinct substitutions of period 30 are given in the following two columns:

1,	2,	27	1,	5,	24
7,	14,	9	7,	5,	18
11,	22,	27	11,	25,	24
13,	26,	21	13,	5,	12
17,	4,	9	17,	25,	18
19,	8,	3	19,	5,	6
23,	16,	21	23,	25,	12
29,	28,	3	29,	25,	6

It was verified that every substitution (1) of period 30 is conjugate in the quotient-group with one of the substitutions whose multipliers are given above.

7. Suppose, lastly, that $p^n - 1 = 3t$, t being divisible by 3. Consider, first, the substitutions C of period $p^n - 1$. Proceeding as in §6, we find that case (c) is now excluded, since $m^2 + m + 1$ is never divisible by 9 and, therefore, not by $3t$. Two cases remain:

(a). As in §6, $m - 1$ must be divisible by t. Setting $m - 1 = kt$, we have $rkt \equiv ct \equiv skt \pmod{3t}$. Since $r - s$ is prime to 3, k must be divisible by 3, whereas $0 < m - 1 < p^n$.

(b). As in §6, we have $m + 1 \equiv 0 \pmod 3$, $m^2 \equiv 1 \pmod{3t}$. Of each pair of solutions $\pm m$ of the latter, one and only one makes $m + 1 \equiv 0 \pmod 3$. Hence there are $2^{\mu+\kappa-1}$ suitable values of m. Inversely, for any such m and any integer r less than and prime to $3t$, the values $s = mr - ct$ $(c = 0, 1, 2)$ make $r - s$ prime to 3, and hence lead to substitutions of period $p^n - 1$. Their multipliers are

$$\alpha, \alpha^m, \alpha^{-1-m}; \ \alpha, \alpha^{m+t}, \alpha^{-1-m-t}; \ \alpha, \alpha^{m-t}, \alpha^{-1-m+t}.$$

---

* In accord with result (c), p. 251, of the earlier paper.

If C_1 denote the substitution corresponding to the first set, the product $C_1^{m-t}\Sigma^m$ has the second set of multipliers and $C_1^{m+t}\Sigma^{-m}$ has the third set of multipliers.

Hence there are only $2^{\mu+\kappa-1}$ *cyclic groups of order* p^n-1; *their generators may be taken to have the multipliers* α, α^m, α^{-1-m}.

These cyclic group are all distinct. In fact, $\alpha^{my}=\alpha$, α^{1+t} or α^{1+2t} requires $y\equiv m \pmod{t}$; $\alpha^{(-1-m)y}=\alpha^{1+ct}$ requires $(m+1)\,y\equiv -1 \pmod{t}$, whereas $m+1$ and t have the common divisor 3. The results may be stated as at the bottom of p. 251 of the earlier paper.

8. It remains to determine the cyclic groups of order $t\equiv\frac{1}{3}(p^n-1)$, t being divisible by 3, which are not contained in any of the cyclic groups of order p^n-1. They may be generated by substitutions C of the form (1) in which $[r, s, 3t]=1$ and $r-s$ is divisible by 3. Inversely, every such substitution C is of period t. By §5, the number of sets r, s, each $<3t$, is $E\equiv 2\,3^{2\tau}F(T)$, where $t=3^\tau T$, T being prime to 3. To determine every substitution C which is conjugate with some of its powers C^m, $1<m<t$, we treat the three cases (*a*), (*b*), (*c*) of §6.

(a). This case is to be excluded since $r\,(m-1)$, $s\,(m-1)$, and, therefore, also $m-1$, must be divisible by t.

(b). Here m^2-1 is divisible by t and, therefore, by 3^τ. Also $r-s\equiv r\,(1-m)+ct$ is divisible by 3, so that $m-1$ is divisible by 3. It follows that $m+1$ is prime to 3 and therefore that $m-1$ is divisible by 3^τ. Inversely, if x be any solution of $x^2\equiv 1 \pmod{T}$ and m be determined by the conditions

$$m\equiv x \pmod{T},\quad m\equiv 1 \pmod{3^\tau},$$

then $m^2\equiv 1 \pmod{t}$ and $m-1$ is divisible by 3. Hence there are $2^{\mu+\kappa-1}-1$ such integers m, $1<m<t$. For each m and r the condition

$$r\,(m^2-1)/t\equiv (m+1)\,c \qquad \pmod{3}$$

determines c modulo 3. If m^2-1 is divisible by $3t$, then $c\equiv 0$; if $m^2-1=(3j\pm 1)\,t$, then $c\equiv \mp r$. In the former case, C has the multipliers

$$\alpha^r,\ \alpha^{mr},\ \alpha^{-r-rm} \qquad [m^2\equiv 1 \pmod{3t}],$$

and is conjugate with C^m. In the latter case, C has the multipliers

$$\alpha^r,\ \alpha^{mr\pm rt},\ \alpha^{-r-mr\mp rt} \qquad [m^2\equiv 1\pm t \pmod{3t}],$$

and is conjugate with C^m in the quotient-group. In either case, C is the r^{th} power of a substitution of period p^n-1 having the distinct multipliers α, α^{m+kt},

$\alpha^{-1-m-kt}$ $(k=0, 1$ or $2)$. *Hence there are* $2^{\mu+\kappa-1}-1$ *of these special cyclic groups of order* t. In all, they contain

$$\tfrac{1}{2}\phi(t)(2^{\mu+\kappa-1}-1)\equiv 3^{\tau-1}\phi(T)(2^{\mu+\kappa-1}-1) \qquad (3)$$

sets of unequal multipliers of substitutions of period t.

(c) Since $r-s\equiv r(1-m)\equiv 0 \pmod 3$, $m-1$ is divisible by 3. Hence, $r(m^2+m+1)$ and, therefore, m^2+m+1 must be divisible by $3t$, whereas, it is not divisible by 9. The case must be excluded.

In $3\,\phi(3t)$ of the E sets r, s, $-r-s$, two of the three integers are equal. The remaining sets give rise to

$$\tfrac{1}{18}[E-3\,\phi(3t)]\equiv 3^{2\tau-2}\phi(T)\,\psi(T)-3^{\tau-1}\phi(T)$$

sets of unequal multipliers of substitutions which are distinct in the quotient-group. Excluding the sets (3), and dividing the resulting number by $\phi(t)$, we obtain

$$\tfrac{1}{2}[3^{\tau-1}\psi(T)-2^{\mu+\kappa-1}],$$

as the number of cyclic groups of order t whose substitutions of period t are never conjugate with any of their powers. In addition to these, there are $2^{\mu+\kappa-1}-1$ special cyclic groups determined above and one cyclic group of order t generated by the substitution with the multipliers α, α, α^{-2}.

Example I.—For $p^n=19$, there are two cyclic G_6 not in the cyclic G_{18} generated by substitutions (1). Their substitutions of period 6 have the multipliers

$$\alpha, \alpha, \alpha^{-2}; \quad \alpha^5, \alpha^5, \alpha^{-10}; \quad \alpha, \alpha^4, \alpha^{13}; \quad \alpha^5, \alpha^2, \alpha^{11}.$$

Example II.—For $p^n=37$, there are four cyclic G_{12} not in the cyclic G_{36}. The multipliers of their substitutions of period 12 are

$$\begin{array}{llll}
\alpha, \alpha, \alpha^{-2}; & \alpha^5, \alpha^5, \alpha^{-10}; & \alpha^7, \alpha^7, \alpha^{-14}; & \alpha^{11}, \alpha^{11}, \alpha^{-22}; \\
\alpha, \alpha^4, \alpha^{-5}; & \alpha^5, \alpha^{-16}, \alpha^{11}; & \alpha^7, \alpha^{-8}, \alpha; & \alpha^{11}, \alpha^8, \alpha^{17}; \\
\alpha, \alpha^{10}, \alpha^{-11}; & \alpha^5, \alpha^{14}, \alpha^{17}; & \alpha^7, \alpha^{-2}, \alpha^{-5}; & \alpha^{11}, \alpha^2, \alpha^{-13}; \\
\alpha, \alpha^{16}, \alpha^{-17}; & \alpha^5, \alpha^8, \alpha^{-13}. & &
\end{array}$$

The last two substitutions are conjugate with their seventh powers.

9. We give a summary of the results of §§3–8, adding the number of conjugate groups of each type. For $p^n=3t+1$, the order N of the simple linear fractional group G is

$$N=\tfrac{1}{3}(p^{3n}-1)(p^{2n}-1)p^{3n}.$$

The substitutions (1) generate cyclic groups which are subgroups of the following system of distinct cyclic groups:

For $t \equiv \frac{1}{3}(p^n - 1)$ prime to 3:

$2^{\mu+\kappa-1}$ sets each of $\dfrac{N}{\frac{2}{3}(p^n-1)^2}$ conjugate G_{p^n-1},

$2^{\delta-1}$ sets each of $N/(p^n-1)^2$ conjugate G_{p^n-1},

$\frac{1}{6}\psi(t) - \frac{1}{3}2^{\delta-1} - \frac{1}{2}2^{\mu+\kappa-1}$ sets each of $N \div \frac{1}{3}(p^n-1)^2$ conjugate G_{p^n-1},

the second set occurring if, and only if, $p^n = 2^n$, n being even and $\frac{1}{3}(2^n-1)$ having only prime factors (δ in number) of the form $6k+1$.

For t divisible by 3:

$2^{\mu+\kappa-1}$ sets each of $N \div \frac{2}{3}(p^n-1)^2$ conjugate G_{p^n-1},

$\frac{1}{2}3^{\tau-1}\psi(T) - \frac{1}{2}2^{\mu+\kappa-1}$ sets each of $N \div \frac{1}{3}(p^n-1)^2$ conjugate G_{p^n-1},

$2^{\mu+\kappa-1} - 1$ sets each of $N \div \frac{2}{3}(p^n-1)^2$ conjugate G_t,

$\frac{1}{2}3^{\tau-1}\psi(T) - \frac{1}{2}2^{\mu+\kappa-1}$ sets each of $N \div \frac{1}{3}(p^n-1)^2$ conjugate G_t,

one set of $N \div \frac{1}{3}(p^{2n}-1)(p^{2n}-p^n)$ conjugate G_t.

THE UNIVERSITY OF CHICAGO, *March*, 1901.